

Notation Index

- \forall (for all) SF-16
- B^A (all functions) SF-16
- $|B^A| = |B|^{|A|}$ (all functions) SF-18
- $(n)_k$ (falling factorial) SF-9
- $a R b$ (binary relation) SF-16
- $C(n, k) = \frac{n!}{k!(n-k)!}$ (binomial coefficient) SF-9
- $n!$ (n factorial) SF-9
- $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ (binomial coefficient) SF-9
- B_n (Bell number) SF-11
- χ (characteristic function) SF-10
- Δ (difference operator) IS-6
- $k \mid n$ (k divides n ; $n/k \in \mathbb{Z}$) NT-2
- $x \equiv y$ (equivalence relation) EO-1
- $\exists!$ (for exactly one) SF-16
- \exists (for some) SF-16
- Function
 - χ (characteristic) SF-10
 - $C(n, k) = \binom{n}{k}$ (binomial coefficient) SF-9
 - $\text{PER}(A) = \mathcal{S}(A)$ (permutations) SF-18
 - $\text{Coimage}(f)$ SF-23
 - $\text{Image}(f)$ SF-23
- Function notation (particular)
 - $\lfloor x \rfloor$ (greatest integer) NT-9
 - $\lceil x \rceil$ (ceiling) NT-9
 - $\text{gcd}(a, b)$ (greatest common divisor) NT-16
 - $\phi(n)$ (Euler ϕ) NT-19
 - $\text{lcm}(a, b)$ (least common multiple) NT-16
- Function notation
 - B^A (all functions) SF-16, SF-17, SF-18
 - $f : A \rightarrow B$ (a function) BF-1, SF-15
 - f^{-1} (inverse, $\neq 1/f$) SF-18
 - $g \circ f$ (composition) SF-20
 - $\text{gcd}(a, b)$ (greatest common divisor) NT-16
 - $\text{lcm}(a, b)$ (least common multiple) NT-16
 - $\exists!$ (for exactly one) SF-16
 - \exists (for some) SF-16
 - \forall (for all) SF-16
 - Logic notation
 - \exists (for some) Lo-13
 - \forall (for all) Lo-12
 - \sim (not) Lo-2
 - \wedge (and) Lo-2
 - \Leftrightarrow (if and only if) Lo-6
 - \vee (or) Lo-2
 - \Rightarrow (if ... then) Lo-5
 - $x \% d$ (x mod d) NT-7
 - \mathbb{N} (Natural numbers) Lo-13, NT-1
 - $\underline{n} = \{1, 2, \dots, n\}$ SF-16
 - $x \prec_C y$ (covering relation) EO-28
 - $x \preceq y$ (order relation) EO-12
 - \mathbb{P} (Prime numbers) Lo-13
 - $\mathcal{P}(A)$ (set of subsets of A) SF-9
 - $\mathcal{P}_k(A)$ (set of k -subsets of A) SF-9
 - $\text{PER}(A) = \mathcal{S}(A)$ (permutations) SF-18
 - \mathbb{Q} (Rational numbers) NT-1
 - \mathbb{R} (Real numbers) Lo-13, NT-1
 - $\Re(z)$ (real part of z) IS-24

Index

Set notation

- $\{x : \dots\}$ (set description) SF-2
- $\{x \mid \dots\}$ (set description) SF-2
- \emptyset (empty set) SF-2
- $\sim A$ (complement) SF-2
- \in and \notin (in and not in) SF-1
- $\times^k A$ (k -fold product) SF-2
- A' (complement) SF-2
- $A - B$ (difference) SF-2
- $A \cap B$ (intersection) SF-2
- $A \cup B$ (union) SF-2
- $A \oplus B$ (symmetric difference) SF-2
- $A \setminus B$ (difference) SF-2
- $A \subseteq B$ (subset) SF-1
- $A \times B$ (Cartesian product) SF-2
- A^c (complement) SF-2
- $\mathcal{P}(A)$ (set of subsets of A) SF-9
- $\mathcal{P}_k(A)$ (set of k -subsets of A) SF-9
- $|A|$ (cardinality) SF-1

Sets of numbers

- \mathbb{N} (Natural numbers) Lo-13, NT-1
- \mathbb{N}^+ (Positive integers) NT-1
- $\mathbb{N}_2^+ (\{n \in \mathbb{Z} \mid n \geq 2\})$ NT-1
- \mathbb{P} (Prime numbers) Lo-13, NT-2
- \mathbb{Q} (Rationals) NT-1
- \mathbb{R} (Real numbers) Lo-13, NT-1
- \mathbb{Z} (Integers) Lo-13, NT-1
- $\underline{n} = \{1, 2, \dots, n\}$ SF-16
- $d\mathbb{Z} + k$ (residue class) NT-6
- $S(n, k)$ (Stirling number) SF-24
- \mathbb{Z} (Integers) Lo-13, NT-1

Subject Index

- Absolute convergence IS-26
- Absorption rule BF-6, Lo-3, SF-3
- Adder
 - full BF-19
 - half BF-18
- Algebraic number theory NT-3
- Algebraic rules for
 - Boolean functions BF-6
 - predicate logic Lo-19
 - sequences IS-16
 - sets SF-2
 - statement forms Lo-3
- Algorithm
 - Euclidean NT-18
- Alternating series IS-24
 - Dirichlet's Theorem IS-24
 - harmonic IS-23
- And form BF-6
- “And” operator ($= \wedge$) BF-3
- Antisymmetric relation EO-13
- Arithmetic
 - binary BF-12
 - computer BF-11
 - modular NT-6
 - two's complement BF-16
- Associative law
 - functional composition SF-20
- Associative rule BF-6, Lo-3, SF-3

- Base case (induction) IS-1
- Base- b number BF-10
 - base change BF-10
 - binary ($=$ base-2) BF-11
 - hexadecimal ($=$ base-16) BF-11
 - octal ($=$ base-8) BF-11
- Bell number SF-11
- Biconditional ($=$ if and only if) Lo-6
- Bijective function SF-18

- Binary number BF-11
 - addition circuit BF-18
 - arithmetic BF-12
 - overflow BF-17
 - register size BF-14
 - two's complement BF-16
- Binary operator BF-3
- Binary relation EO-3
 - direct product of EO-18
- Binomial coefficient
 - Pascal's triangle SF-10
 - recursion SF-10
- Binomial coefficient: $C(n, k) = \binom{n}{k}$ SF-9
- Block of a partition SF-11
- Boolean
 - operator, *see also* operator
 - product ($= \wedge$) EO-27
 - sum ($= \vee$) EO-27
- Boolean function BF-1
 - number of BF-2
 - tabular form BF-1
- Bound rule BF-6, Lo-3
- Bounded sequence IS-16
 - monotone converge IS-17
- Bucket sort EO-22

- Cardinality of a set SF-1
- Cartesian product of sets SF-2
- Ceiling function ($=$ least integer) NT-9
- Chain ($=$ linear order) EO-14
 - length of EO-29
- Characteristic function SF-10
- Ciphertext NT-13
- Circuit for addition BF-18
- Codomain of a function BF-1, SF-15

Index

- Coimage of a function SF-23
 - set partition SF-23
- Commutative rule BF-6, Lo-3, SF-3
- Comparable elements EO-14
- Comparison sort EO-22
- Complement of a set SF-2
- Composite number Lo-13, NT-2
- Composition of functions SF-20, SF-20
 - associative law SF-20
- Computer arithmetic
 - addition circuit BF-18
 - negative number BF-16
 - overflow BF-14, BF-17
 - register size BF-14
 - two's complement BF-16
- Conditional (= if ... then) Lo-5
- Conditional convergence IS-27
- Conjecture
 - Goldbach's Lo-13
 - Twin Prime Lo-16
- Conjunctive normal form BF-6
- Contradiction Lo-2
- Contrapositive Lo-6
- Convergence
 - only tails matter IS-13
 - sequence IS-13
 - sequence — alternate form IS-14
 - sequence — bounded monotone IS-17
 - sequence to infinity IS-19
 - series IS-20
 - series — Abel's Theorem IS-28
 - series — absolute IS-26
 - series — conditional IS-27
 - series — general harmonic IS-25
 - series — integral test IS-24
- Converse Lo-6
- Coordinate order (= direct product) EO-17
- Countable set NT-5
- Covering relation EO-28
- Cryptography NT-13, SF-19
 - Diffie-Hellman protocol NT-22
 - PGP NT-20
 - public key NT-21
 - RSA protocol NT-23
 - symmetric encryption NT-20
 - trapdoor function NT-21
- Cycle form of a permutation SF-22
- Decreasing sequence IS-17
- DeMorgan's rule BF-6, Lo-3, SF-3
- DES (= Data Encryption Standard) SF-19
- Diagonal argument NT-6
- Diagram, Hasse EO-28
- Dictionary order (= lex order) SF-8
- Difference of sets SF-2
 - symmetric SF-2
- Difference operator IS-6
- Diffie-Hellman protocol NT-22
- Digit symbol of index i BF-10
- Direct product of binary relations EO-18
- Direct product of posets EO-17
- Directed graph diagrams EO-26
- Discrete logarithm NT-21
 - Diffie-Hellman and NT-22
- Disjunctive normal form BF-5
- Distributive rule BF-6, Lo-3, SF-3
- Divergence
 - only tails matter IS-13
 - sequence IS-13
 - sequence to infinity IS-19
 - series IS-21
 - series to infinity IS-21
- Divisible by: $k \mid n$ NT-2
- Domain of a function BF-1, SF-15
- Domino coverings EO-24
- Double implication (= if and only if) Lo-6

- Double negation rule BF-6, Lo-3, SF-3
- Element in poset
 - greatest EO-29
 - least EO-29
 - maximal EO-30
 - minimal EO-30
- Element method of proof SF-4
- Elements (of a poset)
 - comparable EO-14
 - incomparable EO-14
- Empty set SF-2
- Encryption SF-19
- English to logic
 - “for all” Lo-12
 - “for some” Lo-13
 - “if and only if” Lo-7
 - method for implication Lo-8
 - “necessary” Lo-7
 - “neither” BF-8
 - “only if” Lo-7
 - “requires” Lo-8
 - “sufficient” Lo-7
 - “there exists” Lo-13
 - “unless” Lo-8
- Envelope game SF-17
- Equivalence class EO-1
- Equivalence relation EO-1
- Espionage NT-15
- Euclidean algorithm NT-18
- Euler ϕ function NT-19
 - RSA protocol and NT-23
- Even integer NT-1
- “Exclusive or” operator ($= \oplus$) BF-3
- Existential quantifier (\exists) Lo-13
- Exponential, rate of growth of IS-18
- Extension, linear EO-30
- Factorial
 - falling SF-9
- Factoring
 - RSA and NT-23
 - uniqueness of NT-3
- Falling factorial SF-9
- Fermat number Lo-16
- Fermat’s Last Theorem Lo-18, NT-3
- Floor function ($=$ greatest integer) NT-9
- For all (logic: \forall) Lo-12
- For some (logic: \exists) Lo-13
- Full adder BF-19
- Function BF-1, SF-15
 - bijective SF-18
 - binomial coefficient: $\binom{n}{k} = C(n, k)$ SF-9
 - Boolean BF-1
 - Boolean, number of BF-2
 - ceiling ($=$ least integer: $\lceil x \rceil$) NT-9
 - characteristic: χ SF-10
 - codomain ($=$ range) of BF-1, SF-15
 - coimage and set partition SF-23
 - coimage of SF-23
 - composition of SF-20, SF-20
 - domain of BF-1, SF-15
 - Euler ϕ NT-19
 - Euler ϕ and RSA protocol NT-23
 - floor ($=$ greatest integer: $\lfloor x \rfloor$) NT-9
 - greatest common divisor ($=$ gcd) NT-16
 - greatest integer NT-9
 - hash SF-19
 - image of SF-15, SF-23
 - injective SF-18
 - inverse SF-18, SF-23
 - least common multiple ($=$ lcm) NT-16
 - least integer NT-9
 - number of SF-18
 - number of $= \binom{n}{k} S(m, k) k!$ SF-25
 - one-line notation for SF-16, SF-16

Index

- one-to-one (= injection) SF-18
- one-way (= trapdoor) NT-21
- onto (= surjection) SF-18
- permutation SF-18
- range (= codomain) of BF-1, SF-15
- surjective SF-18
- trapdoor NT-21
- two-line notation for SF-20, SF-20
- Functional relation SF-16
- Gate BF-18
- Geometric series IS-22
- Goldbach's conjecture Lo-13
- Graph diagrams, directed EO-26
- Greatest common divisor (= gcd) NT-16
 - Euclidean algorithm NT-18
- Greatest element in poset EO-29
- Greatest integer function NT-9
- Half adder BF-18
- Harmonic series IS-22
 - alternating IS-23
 - general IS-25
- Hashing SF-19
- Hasse diagram EO-28
- Hexadecimal number BF-11
- Idempotent rule BF-6, Lo-3, SF-3
- If ... then Lo-5
- If and only if (logic) Lo-7
- Image of a function SF-15, SF-23
- Implication Lo-5
- Incidence matrix EO-14
- Incomparable elements EO-14
- Incomparable subsets EO-14
- Increasing sequence IS-17
- Induction terminology IS-1
- Inductive step IS-1
- Infinite sequence
 - see* Sequence
- Infinite series
 - see* Series
- Injective function SF-18
- Integral test for series IS-24
- Intersection of sets SF-2
- Inverse Lo-6
- Inverse function SF-18
- Inverse relation SF-16
- Irrationality of square root NT-4
- Key (cryptography) NT-13
 - Diffie-Hellman NT-22
 - RSA and public NT-23
 - trapdoor function and NT-21
- Lattice of subsets EO-13
- Least common multiple (= lcm) NT-16
- Least element in poset EO-29
- Least integer function NT-9
- Length-first lex order EO-21
- Lexicographic bucket sort EO-22
- Lexicographic order (= lex order) SF-7, EO-19
 - length-first (= short) EO-21
- Limit
 - of a sequence IS-13
 - sum of infinite series IS-20
- Linear extension EO-30
- Linear order SF-1, EO-14
- List (= ordered set) SF-1
- Logarithm
 - discrete and Diffie-Hellman NT-22
- Logarithm, rate of growth of IS-18
- Logic
 - predicate Lo-12
 - propositional BF-4, Lo-1

- Logic gate BF-18
- Matrix, incidence EO-14
- Maximal element in poset EO-30
- Mersenne number Lo-17
- Minimal element in poset EO-30
- Mod as binary operator NT-7
- Mod as equivalence relation NT-7
- Modular arithmetic NT-6
- Monotone sequence IS-17
- Monotone subsequences EO-8
- Necessary (logic) Lo-7
- Negation rule BF-6, Lo-3
- Normal form
 - conjunctive BF-6
 - disjunctive BF-5
- “Not” operator ($= \sim$) BF-3
- Number
 - base- b BF-10
 - Bell number: B_n SF-11
 - binomial coefficient: $\binom{n}{k} = C(n, k)$ SF-9
 - composite Lo-13, NT-2
 - Fermat: F_n Lo-16
 - integer \mathbb{Z} NT-1
 - integer: \mathbb{Z} Lo-13
 - irrational: $\mathbb{R} - \mathbb{Q}$ NT-1
 - Mersenne: M_p Lo-17
 - natural \mathbb{N} NT-1
 - natural: \mathbb{N} Lo-13
 - perfect Lo-17
 - prime Lo-13
 - prime: \mathbb{P} Lo-13, NT-2
 - rational: \mathbb{Q} NT-1
 - real: \mathbb{R} Lo-13, NT-1
 - square root is irrational NT-4
 - Stirling: $S(n, k)$ SF-24
 - unique prime factorization of NT-3
- Number theory
 - algebraic NT-3
 - elementary Lo-13
 - nonunique factorization NT-3
- Octal number BF-11
- Odd integer NT-1
- One-line notation SF-16, SF-16
- One-to-one function ($=$ injection) SF-18
- One-way ($=$ trapdoor) function NT-21
- Only if (logic) Lo-7
- Onto function ($=$ surjection) SF-18
- Operator
 - and ($= \wedge$) BF-3
 - binary BF-3
 - exclusive or ($= \oplus$) BF-3
 - not ($= \sim$) BF-3
 - or ($= \vee$) BF-3
 - unary BF-3
- Or form BF-5
- “Or” operator ($= \vee$) BF-3
- Order
 - coordinate ($=$ direct product) EO-17
 - dictionary ($=$ lex) SF-8
 - lex ($=$ lexicographic) SF-7
 - lexicographic EO-19
 - linear SF-1
 - relation SF-8
- Order relation EO-12
- Ordered set SF-1
- Overflow BF-14, BF-17
- Partially ordered set
 - see* poset
- Partition of a set SF-11
 - block of SF-11
 - function coimage and SF-23
 - number of SF-11, SF-24
 - refinement of SF-11
- Pascal’s triangle SF-10

Index

- Perfect
 - number Lo-17
- Perfect square NT-4
- Permutation SF-18
 - cycle SF-22
 - cycle form SF-22
 - cycle length SF-22
- PGP (= Pretty Good Privacy) NT-20, SF-19
- Pigeonhole principle EO-5
 - extended EO-7
- Plaintext NT-13
- Polynomial, rate of growth of IS-18
- Poset EO-13
 - comparable elements EO-14
 - coordinate (= direct product) order EO-17
 - covering relation EO-28
 - direct product of EO-17
 - divisibility EO-14, EO-19
 - greatest element EO-29
 - incomparable elements EO-14
 - isomorphic EO-18
 - least element EO-29
 - lex order EO-19
 - linear (= total) order EO-14
 - maximal element EO-30
 - minimal element EO-30
 - restriction of (= subposet) EO-17
 - subset lattice EO-13, EO-17
- Power set SF-9, EO-13
- Powers
 - sum of IS-5
- Predicate logic
 - algebraic rules Lo-19
 - predicate Lo-12
 - quantifier Lo-12
 - truth set Lo-12
- Prime factorization NT-3, IS-2
 - uniqueness of NT-3
- Prime number Lo-13, NT-2
 - how common? IS-28
 - infinitely many NT-4
 - unique factorization into NT-3
- Prime Number Theorem IS-28
- Principle
 - extended pigeonhole EO-7
 - pigeonhole EO-5
- Product of sets SF-2
- Propositional logic BF-4, Lo-1
 - algebraic rules Lo-3
- Public key cryptography NT-21
 - PGP NT-20
 - RSA protocol NT-23
- Quantifier
 - existential (\exists) Lo-13
 - negation of Lo-15
 - universal (\forall) Lo-12
- Range of a function BF-1, SF-15
- Rate of growth IS-18
- Refinement of set partition SF-11, EO-16
- Reflexive relation EO-3, EO-13
- Relation SF-16
 - antisymmetric EO-13
 - binary EO-3
 - covering EO-28
 - equivalence EO-1
 - functional SF-16
 - inverse SF-16
 - number of EO-15
 - order SF-8, EO-12
 - reflexive EO-3, EO-13
 - symmetric EO-3
 - transitive EO-3, EO-13
 - transitive closure of EO-26
- Residue class (modular arithmetic) NT-6
- Restriction of a poset
 - (= subposet) EO-17
- RSA protocol NT-23

Rule

absorption BF-6, Lo-3, SF-3
 associative BF-6, Lo-3, SF-3
 bound BF-6, Lo-3
 commutative BF-6, Lo-3, SF-3
 DeMorgan's BF-6, Lo-3, SF-3
 distributive BF-6, Lo-3, SF-3
 double negation BF-6, Lo-3,
 SF-3
 idempotent BF-6, Lo-3, SF-3
 negation BF-6, Lo-3

Sequence IS-12

algebraic rules for IS-16
 bounded IS-16
 convergent IS-13
 convergent to infinity IS-19
 decreasing IS-17
 divergent IS-13
 divergent to infinity IS-19
 increasing IS-17
 limit of IS-13
 monotone IS-17
 series and IS-20
 tail of IS-12
 term of IS-12

Series IS-20

Abel's Theorem IS-28
 absolute convergence IS-26
 alternating IS-24
 alternating harmonic IS-23
 conditional convergence IS-27
 convergent IS-20
 convergent and small
 terms IS-21
 Dirichlet's Theorem IS-24
 divergent IS-21
 general harmonic IS-25
 geometric IS-22
 harmonic IS-22
 integral test for monotone IS-24
 partial sums IS-20
 sum is a limit IS-20
 tail of IS-20

Set SF-1

algebraic method SF-5
 algebraic rules SF-2
 as a predicate Lo-14
 Bell number: B_n SF-11
 cardinality of SF-1
 Cartesian product SF-2
 characteristic function SF-10
 complement SF-2
 countable NT-5
 difference SF-2
 element method SF-4
 empty SF-2
 intersection SF-2
 number of subsets SF-11
 ordered SF-1
 partially ordered EO-13
 power SF-9, EO-13
 subset SF-1
 symmetric difference SF-2
 union SF-2
 universal SF-1
 Venn diagrams SF-3

Set inclusion order EO-13

Set partition SF-11

block of SF-11
 function coimage and SF-23
 refinement poset EO-16
 refining SF-11
 Stirling number: $S(n, k)$ SF-24

Sort

bucket EO-22
 comparison EO-22
 topological (= linear
 extension) EO-30

Statement form Lo-1

Boolean function and Lo-8

Statement variable BF-3, Lo-1

Stirling number $S(n, k)$ SF-24

String (= ordered set) SF-1

Subposet EO-17

Subset lattice EO-13

Subset of a set SF-1

number of them SF-11

Subset sums EO-6

Index

- Sufficient (logic) Lo-7
- Sum of powers IS-5
- Sums
 - equal EO-6
 - equal subset EO-6
- Surjective function SF-18
- Symmetric difference of sets SF-2
- Symmetric encryption NT-20
- Symmetric relation EO-3

- Tabular form of a Boolean function BF-1
- Tail
 - and convergence IS-13
 - sequence IS-12
 - series IS-20
- Tautology Lo-2
- Term of a
 - sequence IS-12
 - series IS-20
- Theorem
 - Abel's IS-28
 - algebraic rules, *see* Algebraic rules
 - Pigeonhole Principle EO-5
 - Pigeonhole Principle, extended EO-7
 - Prime Number IS-28
 - sequence convergence, *see* Convergence
 - Unique Factorization NT-3
- There exists (logic: \exists) Lo-13
- Tiling problem EO-24
- Topological sort EO-30
- Total order (= linear order) EO-14
- Transitive closure EO-26
- Transitive relation EO-3, EO-13
- Trapdoor function NT-21
 - discrete logarithm NT-22
- Truth set (predicate logic) Lo-12
- Truth table BF-2, BF-4, Lo-2
- Twin Prime conjecture Lo-16

- Two-line notation SF-20, SF-20
- Two's complement BF-16
 - arithmetic BF-16
 - overflow BF-17

- Unary operator BF-3
- Union of sets SF-2
- Unique prime factorization NT-3
- Universal quantifier (\forall) Lo-12
- Universal set SF-1
- Unless (logic) Lo-8

- Vector (= ordered set) SF-1
- Venn diagrams for sets SF-3

- Word (= ordered set) SF-1